UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/826,046	04/04/2001	Charles Steven Lingafelt	RSW920010056US1	2366

26502 7590 03/09/2005

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/826,046	LINGAFELT ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) *4 and 9* is/are allowed.

6)☒ Claim(s) *1-3 and 5-8* is/are rejected.

7)☒ Claim(s) *10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 5, 8, 9 have been amended.
4. New claim 10 has been added.
5. Claims 1-10 are pending.

Response to Arguments

6. Applicant's arguments filed 11/19/2004 have been fully considered but they are not persuasive/ or moot in view of the new ground(s) of rejection.

As per applicant's arguments that "Coley would thus suggest that received message would not pass to the web server, when under attack, because the message would not pass through the verification tests" page 7, first paragraph of the response; and suggesting in the claim invention, that the message containing the source addresses that matched those in the database would be passed to the server are not persuasive for the following reasons:

a) Applicant admits that Coley has two database that contains the authorized list source addresses and un-authorized source addresses (see page 6, last paragraph of Applicant's response. Examiner has considered authorized list as corresponding to Applicant's privileged list of source addresses; and Coley's un-authorized list of source addresses as corresponding to Applicant's blocked list of source addresses as recited in the last office action).

b) Applicant also has admitted that during an attack those messages contain unauthorized source addresses are discarded (blocked) and will not be allowed to be passes to the server (see page 6, last paragraph of Applicant's response).

C) Applicant questions that Coley would not allowed the messages appear on the authorized list to pass to the server unless it passes a verification test. Examiner agrees with this part of Applicant's analogy.

However Examiner differs with Applicant's analogy when it conclude that "Coley would thus suggest that received message would not pass to the web server, when under attack, because the message would not pass through the verification tests" page 7, first paragraph of the response; and suggesting in the claim invention, that the message containing the source addresses that matched those in the database would be passed to the server (implying no verification test needed).

As per applicant's argument with respect to claim 5 that Coley do not disclose "the database of privileged source address" page 7, third paragraph of Applicant's response, examiner refers Applicant to fig.2, item 218 and col.11, lines 27-30 where the list of the "authorized addresses" that corresponds to database of the "privileged source addresses" and list of unauthorized addresses that corresponds to Applicant's database of "blocked source addresses" are maintain in the database of 218 of fig.2);

The question becomes what is the verification test that Coley teach? Col.11, lines 22-40 disclose verification test could be not "little more than verifying address information..". Col.6, lines 33-40 disclose any combination that a verification test could consist of. However the fundamental simplicity of verification is the verification of the addresses information and further verification tests are depend on the type of request access and protocol used (see col.11, lines 38-40; col.6, lines 22-30).

Therefore Applicant's argument has no merit since by Applicant's own admission the source addresses in the message is subjected to a verification test if on the authorized list and as explained above the **simplest** verification test is nothing more than the comparison between the source addresses and the source addresses on the authorized list. In another word if we take the simplest verification test by Coley as our guide as an option then all source addresses received in a message are compared to the authorized list if authenticated it will be passed to the server as set

forth in applicant's claim invention during an ongoing attack since those on unauthorized list are blocked or discarded.

For more detailed please also see col.9, lines 29-31; lines 33-36.

- Examiner agrees with applicant's arguments of claims 4 and 9, and the rejection of claims 4 and 9 has been withdrawn.

Claim Rejections - 35 USC § 102

7. **Claims 1-3 and 5-8** are rejected under 35 U.S.C. 102(b) as being anticipated by Coley et al (5,826,014A).

As per claim 1 Coley et al (5,826,014A) teach a method for improving the operation of equipment used to protect a web server against attack (see fig.4a where a method to protect a web-server against intruder or an attack is demonstrated by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a), comprising the acts of: reading a source address of a message received during an attack (see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a); checking a database of privileged source

addresses (see fig.2, item 218; col.11, lines 27-30 where the comparison of the source address with the list of "authorized addresses" that corresponds to Applicant's privileged source address being conducted and where "the list of the authorized addresses" that maintains by database 218 of fig.2); and instructing protective equipment for a web server to pass the received message to the web server, **regardless of an ongoing attack**, when the source address of the received message matches an address contained in the database of privileged source addresses (see col.11, lines 31-40 where a match between the source address and the address in the authorized list is valid by comparison as shown in step 414 of fig.4a and where after validation connection to the destination in the web server is initiated for sending the message).

Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.

As per claims 2 and 3 Coley et al (5,826,014A) teach the method of claim 1, wherein the database of privileged source addresses includes a source address of a customer/user known to the web server (see fig.2, item 200 and fig.3, items 302 or 300 that corresponds to a customer or a user in conjunction with col.11, lines 27-30 their

address as a source address in being stored in an authorized list for access request; fig.4b disclose further the authentication procedure of a user or a customer for access).

As per claim 5 Coley et al (5,826,014A) teach a Protective equipment for guarding a web server against attack (see fig.2 where a protective equipment such as item 210 firewall is to protect a web-server against intruder or an attack as described in fig.4a by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a), comprising: an address decoder for reading a source address of a message received during an attack (see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a); a database of privileged source addresses (see fig.2, item 218 and col.11, lines 27-30 where the list of the "authorized addresses" that corresponds to "privileged source addresses" and list of unauthorized addresses are maintain in the database of 218 of fig.2); and logic for instructing protective equipment for a web server to pass the message received during the attack to the web server when the source address of the message received during the attack matches a privileged source address contained in the database of privileged source addresses, **regardless of an ongoing attack** (see fig.2, item 18; col.11, lines 27-30 where the comparison of the source address with the list of authorized addresses

that corresponds to Applicant's privileged source address being conducted where the list of the authorized addresses that maintain; see col.11, lines 31-40 where a match between the source address and the address in the authorized list is valid by comparison as shown in step 414 of fig.4a then connection to the destination is initiated for sending the message).

Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.

As per claims 6 and 7 Coley et al (5,826,014A) teach the intrusion detection security system of claim 5, wherein the database of privileged source addresses includes a source address of a customer/user known to access the web server (see fig.2, item 200 and fig.3, items 302 or 300 that corresponds to a customer or a user in conjunction with col.11, lines 27-30 their address as a source address in being stored in an authorized list for access request; fig.4b disclose further the authentication procedure of a user or a customer for access).

As per claim 8 Coley et al (5,826,014A) teach a Protective equipment for guarding a web server against attack (see fig.4a where a method to protect a web-server against

intruder or an attack is demonstrated by source address, service and time verification where a failure result in deny access to the web-server; col.5, lines 49-52 disclose the firewall is resistant to attack and col.6, lines 4-21 disclose a method of operation to protect a web-server of fig.4a), comprising: an address decoder for reading a source address of a message received during an attack (see fig.4a, step 412 where the step requires checking the source address information where checking corresponds to Applicant's reading of the source address; col.11, lines 22-25 disclose analyzing of the source address for determining access to the web server by reading the source address as shown in step 412 of fig.4a); a database of privileged source addresses, **which passes a packet containing a privileged source address to the web server regardless of an ongoing attack**; a database of blocked source addresses (see fig.2, item 218 and col.11, lines 27-40 where the list of the "authorized addresses" that corresponds to "privileged source addresses" and list of "unauthorized addresses" that corresponds to "blocked addresses" are maintain in the database 218 of fig.2 and where the packets that their source address matches the authorized list of source addresses allowed to pass to the server); and logic for checking the database of privileged source addresses and the database of blocked source addresses for appearance of the source address of the message received during the attack and, responsive to the appearance, instructing protective equipment to block incoming message that bear the source address of the message received during the attack (see fig.4a, item 412, 414 and 416; col.11, lines 27-33 where the comparison of the source address with the list of authorized addresses that corresponds to Applicant's privileged source address and list

of unauthorized addresses that corresponds to block source addresses being conducted and in case of invalidation address it block the access by deny access message).

Examiner also refers Applicant to col.13, lines 46-57 where Coley's method where of operation of computing system as described above can take the form of a medium for controlling such a system, or article of manufactures as machine readable medium or computer readable program code which causes a computing system upon which the firewall program system is running to function, and that is any hardware or logical circuit or function that enables the above process to run and function.

Allowable Subject Matter

8. Claims 4 and 9 are allowed.

9. Claim 10 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see

http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

03/04/2005